PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-056037
(43)Date of publication of application : 05.03.1993

(51)Int.Cl. H04L 9/28
G06K 17/00
G09C 1/00

(21)Application number : 03-240374
(22)Date of filing : 27.08.1991

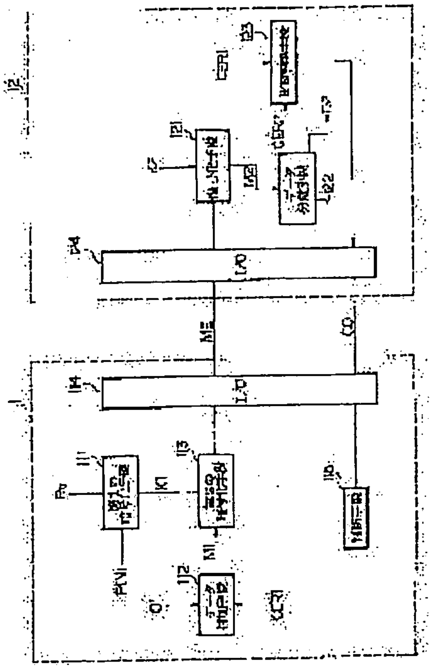
(71)Applicant : TOPPAN PRINTING CO LTD
(72)Inventor : TAKAHASHI MASASHI
YORIMOTO GIICHI
YURA AKIYUKI

(54) DATA PROCESSING SYSTEM

(57)Abstract:

PURPOSE: To reduce the processing time without deteriorating the secrecy of data in the data transmission system between an IC card and a terminal equipment.

CONSTITUTION: A password PIN1 inputted by a carrier of an IC card 12 is ciphered according to a predetermined key data Rd to generate a key data K1. A synthesis text data M1 resulting from adding an additional data CER1 to a text data D1 representing a deposit balance or the like is ciphered according to the key data K1 to generate a ciphered text data ME. The ciphered synthesis text data ME has information comprising the text data D1 and the password PIN1. The ciphered synthesis text data ME is decoded and separated into a text data D2 and an additional data CER2. The separated additional data CER2 is compared with the additional data CER1 stored in advance in the IC card 12. As a result, the adequacy of the correlation PIN1 and the text data D2 is judged. Then the number of times of ciphering/decoding and the number of times of data transmission reception between the terminal equipment 11 and the IC card 12 are reduced to reduce the time required for session.



LEGAL STATUS

[Date of request for examination]	22.06.1998
[Date of sending the examiner's decision of rejection]	16.10.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

JPO and NCIPI are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] By enciphering wording-of-a-telegram data with transmitting-side equipment, transmitting the this enciphered wording-of-a-telegram data to receiving-side equipment, and decrypting the wording-of-a-telegram data this enciphered with receiving-side equipment In the data-processing method which sends and receives these wording-of-a-telegram data the above-mentioned transmitting-side equipment A data addition means to add discernment data to the above-mentioned wording-of-a-telegram data, and to generate synthetic wording-of-a-telegram data, The 1st encryption means which enciphers with the 1st key data which was able to define the password code beforehand, and generates the 2nd key data, While having the 2nd encryption means which enciphers the above-mentioned synthetic wording-of-a-telegram data with the key data of the above 2nd, and generates code composition wording-of-a-telegram data, and a transmitting means to transmit the above-mentioned code composition wording-of-a-telegram data to the above-mentioned receiving-side equipment A receiving means to receive the code composition wording-of-a-telegram data with which the above-mentioned receiving-side equipment was transmitted from the above-mentioned transmitting means, A decryption means to decrypt the above-mentioned code composition wording-of-a-telegram data according to the 3rd key data corresponding to the key data of the above 2nd, and to generate decode composition wording-of-a-telegram data, A data separation means to divide the above-mentioned decode composition wording-of-a-telegram data into decode wording-of-a-telegram data and decode discernment data, When the above-mentioned decode addition data are compared with the above-mentioned addition data and the above-mentioned decode addition data and the above-mentioned addition data are in agreement, the above-mentioned password code, And it is the data-processing method characterized by having a comparative judgment means to judge that the above-mentioned password code and the above-mentioned decode wording-of-a-telegram data are inaccurate when it judges that the above-mentioned decode wording-of-a-telegram data are just and the above-mentioned decode addition data and the above-mentioned addition data are not in agreement.
[Claim 2] The key data of the above 3rd are a data-processing method according to claim 1 characterized by it being generated beforehand and coming to be held with an authorization code and the 1st key data at the store of the above-mentioned receiving-side equipment.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to a data-processing method and the data-processing method which protects the confidentiality of the commo data used in an IC card and a card data processor in detail.
[0002]
[Description of the Prior Art] Conventionally, in the field of an information communication link, techniques, such as encryption of communication link wording of a telegram and electronic signature, have been used as a means to prevent the so-called security risks, such as tapping of the communication link wording of a telegram by the malfeasance, and forgery. For example, data-processing methods, such as "the approach of transmitting secret data between a sending set and a receiving set, equipment", etc. which are shown in the open patent official report No. 136058 [Showa 56 to], have been thought out.
[0003] Drawing 3 is the outline block diagram showing an example of such a conventional data-processing method. This data-processing method has a terminal (transmitting side) 31 and IC card (receiving side) 32, and is constituted. If, as for this data-processing method, IC card 32 holder inputs the password code PIN 1 into a terminal 31, the wording-of-a-telegram data D1, such as the deposits-and-savings balance, will be written in IC card 32 as wording-of-a-telegram data D2 at IC card 32.
[0004] In a terminal 31, the standard key data R which can change the value at random are enciphered by the encryption means 311, and the proper key data R1 are generated. It is transmitted by the transceiver means 316 and this standard key data R is inputted into the encryption means 321 through the transceiver means 326 of IC card 32. This encryption means 321 generates the proper key data R2 based on the standard key data R.
[0005] By changing this standard key data R into each session (data communication between a terminal and an IC card) of every at random, it made it difficult that the proper key data R1 and R2 were known by the third party, and unjust acts, such as tapping of wording-of-a-telegram data D1 grade and forgery of IC card 32, are prevented. Moreover, also when the proper key data R1 and R2 are known by the third party in a certain session, since the standard key data R are changed at random, even the proper key data R1 and R2 in other sessions should not be known.
[0006] Then, in a terminal 31, the password code PIN 1 is enciphered considering the above-mentioned proper key data R1 as a key by the encryption means 312, and the code password code AV1 is generated. This code password code AV1 is inputted into the decryption means 322 through the transceiver means 316 and the transceiver means 326. Then, the code password code AV1 is decrypted considering the above-mentioned proper key data R2 as a key, and the password code PIN 2 is generated. The comparison means 323 compares the decrypted password code PIN 2 with the password code PIN 1 in which it was beforehand stored by IC card 32. And as a result of meaning whether the password code PIN 2 is in agreement with the password code PIN 1, IC card 32 outputs data C1 to a terminal 31.
[0007] The result data C1 are inputted into the decision means 313 through the transceiver means 326 and 316. When it is judged that the password code PIN 2 of the decision means 313 does not correspond with the password code PIN 1 from the result data C1, the session concerned is interrupted and IC card 32 is discharged from a terminal 31. On the other hand, when the password code PIN 2 was in agreement with the password code PIN 1 and the decision means 313 judges, it is carried out by the next processing continuing.
[0008] The wording-of-a-telegram data D1 are enciphered by the encryption means 314 by using the above-mentioned proper key data R1 as a key, and the encryption wording-of-a-telegram data DE are generated. The encryption wording-of-a-telegram data DE are inputted into the decryption means 324 through the transceiver means 316 and 326. The encryption wording-of-a-telegram data DE are decrypted by the decryption means 324 by using the above-mentioned proper key data R2 as a key, and the wording-of-a-telegram data D2 are generated.
[0009] The wording-of-a-telegram data D2 are written in the memory in IC card 32 (not shown). The decision means 325 judges whether processing of the writing of the wording-of-a-telegram data D2 etc. was performed normally, and transmits the result data C2 to the decision means 315 through the transceiver means 315 and 326. As a result of decision, if processing of the writing of the wording-of-a-telegram data D2 etc. is normal, the session processing concerned will be ended, and if not normal, IC card 32 will be discharged from a terminal 31.
[0010] In addition, in the above-mentioned encryption means 312 and 314 and the decryption means 322 and 324, encryption algorithms, such as DES (Data Encryption Standard), FEAL, and RSA, are used.
[0011]

[Problem(s) to be Solved by the Invention] However, in the conventional data-processing method, CPU of the comparatively late 8-bit class of processing speed is mainly carried in the IC card which is a receiving side from constraint of mounting space etc. For this reason, when processing shown in the data-processing method concerning the above-mentioned conventional technique was performed, there was a problem that it was not suitable for practical use that there are many counts of that there are many counts of transmission of wording-of-a-telegram data, encryption, and a decryption in order to require long duration (several seconds) as that processing time as a whole. Moreover, for the object which shortens the processing time, when a simple method realized a data-processing method, the confidentiality of data, such as wording-of-a-telegram data, an authorization code, and proper key data, fell, and the problem of becoming easy to generate a security risk had arisen.

[0012]

[Objects of the Invention] Then, this invention sets it as the object to offer the data-processing method which can shorten the processing time, without reducing the confidentiality of data.

[0013]

[Means for Solving the Problem] The data-processing method concerning invention according to claim 1 By enciphering wording-of-a-telegram data with transmitting-side equipment, transmitting the this enciphered wording-of-a-telegram data to receiving-side equipment, and decrypting the wording-of-a-telegram data this enciphered with receiving-side equipment In the data-processing method which sends and receives these wording-of-a-telegram data the above-mentioned transmitting-side equipment A data addition means to add discernment data to the above-mentioned wording-of-a-telegram data, and to generate synthetic wording-of-a-telegram data, The 1st encryption means which enciphers with the 1st key data which was able to define the password code beforehand, and generates the 2nd key data, While having the 2nd encryption means which enciphers the above-mentioned synthetic wording-of-a-telegram data with the key data of the above 2nd, and generates code composition wording-of-a-telegram data, and a transmitting means to transmit the above-mentioned code composition wording-of-a-telegram data to the above-mentioned receiving-side equipment A receiving means to receive the code composition wording-of-a-telegram data with which the above-mentioned receiving-side equipment was transmitted from the above-mentioned transmitting means, A decryption means to decrypt the above-mentioned code composition wording-of-a-telegram data according to the 3rd key data corresponding to the key data of the above 2nd, and to generate decode composition wording-of-a-telegram data, A data separation means to divide the above-mentioned decode composition wording-of-a-telegram data into decode wording-of-a-telegram data and decode discernment data, When the above-mentioned decode addition data are compared with the above-mentioned addition data and the above-mentioned decode addition data and the above-mentioned addition data are in agreement, the above-mentioned password code, And when it judges that the above-mentioned decode wording-of-a-telegram data are just and the above-mentioned decode addition data and the above-mentioned addition data are not in agreement, it is the data-processing method characterized by having the above-mentioned password code and a comparative judgment means to judge that the above-mentioned decode wording-of-a-telegram data are inaccurate.

[0014] Data-processing method concerning invention according to claim 2 It is the data-processing method according to claim 1 characterized by the key data of the above 3rd being generated beforehand and coming to hold them with an authorization code and the 1st key data at a store.

[0015]

[Function] In a transmitting side, the data-processing method concerning invention according to claim 1 enciphers an authorization code according to the 1st (determined according to card) key data defined beforehand, and generates the 2nd key data. Moreover, addition data are added to the wording-of-a-telegram data in which the content which should be transmitted is shown, and synthetic wording-of-a-telegram data are generated. And this synthetic wording-of-a-telegram data is enciphered based on the key data of the above 2nd, and code composition wording-of-a-telegram data are generated. This code composition wording-of-a-telegram data is transmitted to a receiving side through a transmitting means.

[0016] In a receiving side, the above-mentioned code composition wording-of-a-telegram data are received through a receiving means. This code composition wording-of-a-telegram data is decrypted with the 3rd key data, and generates decode composition wording-of-a-telegram data. This decode composition wording-of-a-telegram data is divided into decode wording-of-a-telegram data and decode discernment data. When this decode discernment data is compared with the above-mentioned discernment data and the above-mentioned decode discernment data and the above-mentioned discernment data are in agreement, it is judged that the above-mentioned authorization code and the above-mentioned decode wording-of-a-telegram data are just. Then, this wording-of-a-telegram data will be written in the IC card which is receiving-side equipment, for example. On the contrary, when the above-mentioned decode discernment data and the above-mentioned discernment data are not in agreement, it is judged that the above-mentioned authorization code and the above-mentioned decode wording-of-a-telegram data are inaccurate. In this case, wording-of-a-telegram data are not written in an IC card.

[0017] Thus, in order to encipher wording-of-a-telegram data with discernment data and to transmit, the routine which transmits only an authorization code apart from transmission of wording-of-a-telegram data, and performs the authentication like before can be omitted, and the effectiveness of transmission of wording-of-a-telegram data is raised. Moreover, since discernment data and wording-of-a-telegram data are enciphered and decrypted simultaneously, the step of encryption and a decryption also decreases compared with the conventional case, and the effectiveness of the data transmission processing is raised. Furthermore, since the authorization code of a proper was used for the receiving side in this case and wording-of-a-telegram data are enciphered, the security about wording-of-a-telegram data which transmits is raised even to the same extent as the case where it is presupposed that the conventional standard key is changed for every session.

[0018] Data-processing method concerning invention according to claim 2 With an authorization code and the 1st key data, the key data of the above 3rd are generated beforehand and held at the storage of the above-mentioned receiving-side equipment. For this reason, it is not necessary to transmit the key data of the above 3rd to receiving-side equipment from transmitting-side equipment, and the time amount which a session takes can be shortened.

[0019]

[Example] Below, the example of this invention is explained, referring to a drawing.

[0020] Drawing 1 is the block diagram showing the outline of the data-processing method concerning the 1st example of this invention. This data-processing method has a terminal (transmitting side) 11 and IC card (receiving side) 12, and is constituted. This example explains the case where the terminal by which online connection was made considering for example, the ATM card for banks as a terminal at the host computer of a bank is used as IC card 12. In this case, an authorization code shall be the thing of a different proper for every card, and only the card holder shall know it. Therefore, hereafter, a card holder inputs authorization code PIN1 into a terminal 31, a terminal performs further predetermined actuation, and the case where the credit of the fixed amount of money is drawn out is explained. Credit cash-drawer processing needs to be performed with a terminal and a host computer, and the credit balance needs to calculate it, and it needs to write this credit balance in a card. Consequently, the wording-of-a-telegram data D1 in which the credit balance and its writing are shown from a host computer are transmitted to a terminal 31, and a terminal transmits this wording-of-a-telegram data to an IC card.

[0021] In the terminal 11 which constitutes transmitting-side equipment, it has the 1st encryption means 11. This 1st encryption means 11 enciphers inputted authorization code PIN1 according to the key data Rd which are the code of the secrecy determined at the time of card issuance, and generates the key data K1. Moreover, this 1st encryption means 11 is constituted by using the encryption algorithm exhibited [RSA / DES, FEAL,].

[0022] Moreover, a terminal 11 adds the discernment data CER1 to the above-mentioned wording-of-a-telegram data D1, has a data addition means 112 to generate the synthetic wording-of-a-telegram data M1, the 2nd encryption means 113 which enciphers the synthetic wording-of-a-telegram data M1, and generates the code composition wording-of-a-telegram data ME, and the transceiver means (I/O circuit) 114 which transmit and receive data between IC cards 12, and is constituted. The same open mold encryption algorithm as the encryption means of the above 1st also constitutes the 2nd encryption means 113.

[0023] On the other hand, IC card 12 is constituted including 8-bit CPU etc., and this CPU is performing processing shown by the following processing means. Namely, a transceiver means 124 by which IC card 12 transmits and receives data between terminals 11 (I/O circuit), A decryption means 121 to decrypt code composition wording-of-a-telegram data according to the key data K2 which were able to be defined beforehand, and to generate the synthetic wording-of-a-telegram data M2, A data separation means 122 to divide the synthetic wording-of-a-telegram data M2 into the wording-of-a-telegram data D2 and the discernment data CER2, The discernment data CER2 are compared with the discernment data CER1, and authorization code PIN1 and the wording-of-a-telegram data M2 have a comparative judgment means 123 to judge whether it is the right, and are constituted. Furthermore, although not illustrated, this IC card 12 has EEPROM in which data, such as the above-mentioned credit balance, were stored, and is constituted.

[0024] The above-mentioned decryption means 121 can process the inverse function of the above-mentioned encryption means 113, and these decryption means 121 and the encryption means 113 can use encryption algorithms, such as DES, FEAL, and RSA, like the above. Moreover, the processing in the above-mentioned data addition means 112 and the data separation means 122 may use what kind of mode of processing, as long as the wording-of-a-telegram data D2 and the discernment data CER2 are disengageable.

[0025] In addition, the above-mentioned terminal has the decision means 115, this decision means judges forward [of wording-of-a-telegram data and an authorization code], and injustice based on the response from the above-mentioned IC card, for example, when inaccurate, a right case orders it the blowdown processing from the terminal of the IC card concerned etc., while outputting that to a host computer.

[0026] Next, an operation of the data-processing method concerning this example is explained, referring to the flow chart of drawing 2 . In this flow chart, S201-S204 show the processing by the side of a terminal 11, and S205-S211 show the processing by the side of an IC card.

[0027] Authorization code PIN1 is inputted into a terminal 11 by the IC card holder. According to the key data Rd determined at the time of card issuance, it enciphers with the encryption means 111, and authorization code PIN1 generates the key data K1 (S201). And about the wording-of-a-telegram data D1 in which the credit balance from a host computer etc. is shown, the discernment data CER1 are added to the wording-of-a-telegram data D1 with the data addition means 112 (for example, a parity bit is added), and the synthetic wording-of-a-telegram data M1 are generated (S202).

[0028] Furthermore, this synthetic wording-of-a-telegram data M1 is enciphered according to the above-mentioned key data K1, and the code composition wording-of-a-telegram data ME are generated (S203). This code composition wording-of-a-telegram data ME is transmitted to IC card 12 through the transceiver means 114 (S204). Consequently, IC card 12 receives this code composition wording-of-a-telegram data through the transceiver means 124.

[0029] The received code composition wording-of-a-telegram data ME are decrypted by the decryption means 121 according to the key data K2, and the synthetic wording-of-a-telegram data M2 are generated (S205). The key data K2 have the value corresponding to the above-mentioned key data K1, and the decryption means 121 performs decryption processing according to the operations sequence of the above-mentioned encryption means 113 and reverse. In addition, the key data K2 can also use data equivalent to the above-mentioned key data K1, and you may make it receive this key data K2 from a terminal 11 after session initiation by using the encryption algorithm of object key methods, such as DES. Furthermore, the key data K2 enciphered with the key data Rd which are the 1st key data beforehand set up according to each card in the authorization code (personal identification number) which may store in IC card 12 the value defined at the time of issuance of IC card 12, for example, is inputted at the time of each card issuance may be beforehand stored in IC card 12. Since the count of transmission and reception of the data of a terminal 11 and IC card 12 becomes fewer when the key data K2 are stored in IC card 12, much more high-speed processing can be aimed at.

[0030] Furthermore, this synthetic wording-of-a-telegram data M2 is separated into the wording-of-a-telegram data D2 and the discernment data CER2 by the data separation means 122 (S206). The comparative judgment means 123 compares the separated discernment data CER2 with the discernment data CER1 in which it was stored by IC card 12 at the time of IC card issuance (S207). In addition, the discernment data CER1 stored in IC card 12 are equivalent to the discernment data CER1 stored in the above-mentioned terminal 11.

[0031] As a result of a comparison, when the separated discernment data CER2 are in agreement with the discernment data CER1, YES), above-mentioned authorization code PIN1, and the wording-of-a-telegram data D2 are judged to be the rights by (S207 (S208). Consequently, as a result of showing normal processing, the wording-of-a-telegram data D2 in which this credit balance is shown transmit data C0 to the transceiver means 114 through the transceiver means 124, while being written in EEPROM of IC card 12 (S209). As a result, the decision means 115 terminates the session of IC card 12 and a terminal 11 according to data C0.

[0032] As a result of a comparison, when the separated discernment data CER2 are not in agreement with the discernment data CER1, it is judged by (S207 that NO), above-mentioned authorization code PIN1, and the wording-of-a-telegram data D2 are not right (S210). That is, authorization code PIN1 judges that the not an authorization code but wording-of-a-telegram data D2 of IC card 12 in the session concerned differ from the wording-of-a-telegram data D1 as a result processed with the host computer. Therefore, without writing this wording-of-a-telegram data D2 in IC card 12, as a result of showing exception processing, data C0 are transmitted to the transceiver means 114 through the transceiver means 124. Consequently, the decision means 115 discharges IC card 12 from a terminal 11 (S211), and a session is terminated. Consequently, the unjust writing to IC card 12 is prevented.

[0033] As mentioned above, as explained, in this example, it enciphers according to the key data K1 which generated the wording-of-a-telegram data D1 from authorization code PIN1, and the code composition wording-of-a-telegram data ME are generated. Therefore, in addition to the wording-of-a-telegram data D1, the code composition wording-of-a-telegram data ME will also have the information on authorization code PIN1. For this reason, the data-processing method concerning this example does not need to perform encryption and a decryption for authorization code PIN1 and the wording-of-a-telegram data D1 independently, as performed by the conventional data-processing method. Moreover, as compared with the conventional data-processing method, transmission and reception of the data between a terminal and an IC card decrease from 4 times to 2 times, and the count of encryption and a decryption is decreasing the data-processing method concerning this example from 6 times to 2 times. Therefore, according to this example, the time amount which the session between a terminal and an IC card takes can be substantially decreased from Number sec to hundreds msec(s).

[0034] Moreover, the key data K1 are generated by enciphering different authorization code PIN1 for every IC card. For this reason, since the key data K1 of other IC cards 12 will not be known even if authorization code PIN1 of IC card 12 of one sheet is known by the third party, the confidentiality of the data of other IC cards 12 does not fall. Therefore, it is not spoiled to the confidentiality of the data of other IC cards, and the damage by the so-called security risk can be suppressed to the minimum. Furthermore, also when a third party acquires others' IC card 12, if a third party does not know the authorization code of this IC card, the data encryption and the decryption are impossible.

[0035] Therefore, the data-processing method concerning this example can shorten the time amount which a session takes, without reducing the confidentiality of data as compared with the conventional data-processing method.

[0036]

[Effect of the Invention] The data-processing method which can shorten the processing time can be offered without reducing the confidentiality of data according to this invention, as explained above.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the outline block diagram showing the data-processing method concerning the 1st example of this invention.
[Drawing 2] It is the flow chart which shows actuation of the data-processing method concerning the 1st example of this invention.
[Drawing 3] It is the outline block diagram showing an example of the conventional data-processing method.
[Description of Notations]
11 Terminal System (Transmitting Side)
12 IC Card (Receiving Side)
111 1st Encryption Means
112 Data Addition Means
113 2nd Encryption Means
114 Transceiver Means (Transmitting Means)
121 Decryption Means
122 Data Separation Means
123 Comparative Judgment Means
124 Transceiver Means (Receiving Means)
D1 Wording-of-a-telegram data
D2 Wording-of-a-telegram data (decode wording-of-a-telegram data)
PIN1 Authorization code
CER1 Discernment data
CER2 Discernment data (decode discernment data)
M1 Synthetic wording-of-a-telegram data
M2 Synthetic wording-of-a-telegram data (decode composition wording-of-a-telegram data)
Rd Key data (1st key data)
K1 Key data (2nd key data)
K2 Key data (3rd key data)

[Translation done.]